Comments on the Federal Trade Commission's Proposal for Behavioral Advertising Principles

Jason Carmel
Senior Optimization Manager
jasonc@zaaz.com

12 February 2008

ZAAZ

414 OLIVE WAY, SUITE 500 SEATTLE, WA 98101

INTRODUCTION

ZAAZ is pleased to present you with our comments on the Federal Trade Commission's Proposal for Behavioral Advertising Principles.

As an industry-leading practitioner of Behavioral Targeting, Site-side optimization, and Web Analytics[1], ZAAZ understands the complexity of issues surrounding the advent of Behavioral Targeting both in terms of the benefits to businesses and consumers, as well as the valid causes for privacy concern.

It is our hope that ZAAZ can partner with the FTC to help foster a system where consumers are able to take advantage of a more personalized and relevant Internet while still maintaining a reasonable expectation of privacy.

About ZAAZ

ZAAZ helps the world's most powerful brands grow and thrive online with performance-driven design, analytics, and optimization services. As a full service interactive agency, ZAAZ provides web strategy, design, development, user experience, analytics, and optimization to Global 1000 companies including Microsoft, Sony Electronics, PR Newswire, Tom's of Maine, Ford Motor Company, Converse, and others. Founded in 1998, ZAAZ has offices in Seattle, Portland, Detroit, San Francisco, and Chicago. ZAAZ is a member of the Wunderman Network and part of the WPP group of companies. For more information, visit www.zaaz.com.

[1] Burns, M. (2007). *Where To Get Help With Web Analytics.* Cambridge: Forrester.

ZAAZ

414 OLIVE WAY, SUITE 500 SEATTLE, WA 98101

ZAAZ RESPONSE TO PROPOSED PRINCIPLES

Behavioral Advertising/Targeting represents a significant advancement for both businesses and consumers relative to blanket advertising. Businesses save money by advertising directly to consumers who are most likely to be interested in their goods and services, while consumers benefit from receiving advertising content that is more relevant to their interests as opposed to randomly distributed advertisements blasted indiscriminately across a network. If one assumes that advertising across and within websites continues to grow as a pillar of Internet revenue[2], then the FTC must take great care to balance the interests of consumers against the risk of unnecessarily stifling growth and innovation.

General Response Themes

As a practitioner of Behavior Targeting for our clients, ZAAZ urges the FTC to develop in more detail the definitions within the proposed Principles to minimize the likelihood of ambiguity. The current Principles demonstrate a possible confusion between various distinct practices all lumped within the catch-all category of Behavioral Marketing. Without adequate definitions, the FTC risks placing undue burdens on both consumers and businesses without any real protection or benefit. As such, ZAAZ recommends re-framing the Principles with the following themes in mind:

The FTC must differentiate between ad-side Behavioral Targeting and site-side Behavioral Targeting – ZAAZ, as well as other industry leaders, recognize and practice multiple types of Behavioral Targeting, defined into two broad categories of site-side and ad-side.[3] Ad-side Behavioral Targeting uses advertising network assets to track a visitor's path across multiple sites for the purpose of presenting relevant content and advertising on the Targeter's site. Thus, an online book seller who employs ad-side Behavioral Targeting may wish to have ads placed on a third party site with a high cluster of likely purchasers (e.g., a travel site) and would consequently wish to highlight items that coincide with those web pages when they visit (e.g., presenting those customers with the travel books). Given its ability to map a path of a visitor across multiple sites, it is ad-side targeting that is the subject of the majority of privacy concerns.[4] Site-side Behavioral Targeting uses referring source, technographics, previous visit information and path tracking self-contained within the Targeter's site to provide similarly relevant content and advertising. This type of Behavioral Targeting is focused on web analytics and data mining within a single web property rather than across the Internet at large.[5] Thus, that same book seller would look at previous

[2] Interactive Advertising Bureau. (2007, November 12). *Internet Advertising Revenues in Q3 '07 Surpass $5.2 Billion, Setting New High.* Retrieved January 14, 2008, from IAB.net: http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/64544

[3] Kaufman, A. (2007, April 9). *Moving Beyond Event-Based Targeting.* Retrieved January 16, 2008, from imedia connection: http://www.imediaconnection.com/content/14391.asp

[4] White, B. (2007, December 6). Watching What You See on the Web. *The Wall Street Journal* , p. B1.

[5] Person, R. (2005, February 15). *The Other Side of Behavioral Targeting.* Retrieved January 14, 2008, from iMedia Connection: http://www.imediaconnection.com/content/5070.asp

ZAAZ

414 OLIVE WAY, SUITE 500 SEATTLE, WA 98101

purchases by a visitor on that same site to suggest related books that the visitor might enjoy, rather than garnering that information based on visits to external, unaffiliated sites. Virtually all companies with an e-commerce presence engage in some form of site-side Behavioral Targeting. Because site-side Behavioral Targeting is used by a website for that website based on information acquired through a visitor's relationship directly with that website, ZAAZ believes this type of marketing is radically different from its ad-side sister, and that general principles designed to address both are likely to create confusion and unnecessarily restrict acceptable business practices.

The FTC should avoid undue burden for online marketing – Given the transparent nature of the technology and the efficiencies of scale, it is tempting to call for restrictions of online Behavioral Targeting specifically despite the existence of legitimate and relatively unregulated analogues in the offline world. Previous purchases are recorded as a matter of course at super markets through the mechanism of "coupon cards" and used to offer specific incentives to shoppers, just as airlines rely on mileage plans to alert travelers to special offers. Online Behavioral Targeting must track to the same standards as offline equivalents.

The FTC must encourage self-regulation, and should rely on Market Pressure as a deterrent wherever possible - ZAAZ is a proponent of privacy online and self-regulates in all business engagements according to a strict, internal set of ethical standards (ZAAZ Values) that prize trust, integrity and perspective over an all-out pursuit of business goals. In the nine year history of the agency, ZAAZ has learned that a policy of honesty and openness with clients, their customers, and vendors results in customer loyalty and a positive reputation within the industry. Conversely, even the brief history of the Internet is replete with examples where a failure to provide adequate safeguards for customer data resulted in public relations nightmares, subsequent mass migrations of customers to competitors, and skyrocketing expenses associated with remedying breached systems.[6] In an effort to avoid these mistakes, businesses who engage in targeting of any kind are learning to exceed the comfort zones of their customers only at their own economic peril. Providing the actions of a business that abuse the trust of its customers do not rise to a violation of existing law, the FTC should defer to customers themselves to punish or reward business behavior with defection or continued patronage.

When self-regulation fails, the FTC should defer to existing rules and laws wherever possible – Lawmakers have responded to a growing concern among their constituents about privacy abuses with a series of regulations designed to protect individuals against the dissemination of private information. The Federal government,

[6] Westervelt, R. (2006, October 31). *Survey: Data breach costs surge.* Retrieved January 14, 2008, from SearchSecurity.com: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1227119,00.html

ZAAZ

in many cases, already has these laws in place to protect against the misappropriation and/or dissemination of confidential, sensitive data that the proposed Principles might address (See e.g., the Federal Standards for Privacy of Individually Identifiable Health Information (HIPAA)[7], the Gramm-Leach-Bliley Act (GLBA) for financial information[8], the Fair Credit Reporting Act for credit information[9], and the Children's Online Privacy Protection Act (COPPA)[10] for information collected from children). These laws may represent a more mature and fine-tuned starting point for any regulation of confidential information across the Internet. ZAAZ recommends maintaining strict enforcement of existing laws or expansion of those laws where appropriate to protect these most sensitive data sets.

Response to Specific Proposals

Regarding the specific Principles suggested by the Federal Trade Commission, ZAAZ respectfully submits the following comments:

Principle #1 - Transparency and Consumer Control

"Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option."

ZAAZ agrees with this principle for the purposes of site-side Behavioral Targeting, and suggests that a comprehensive and available Privacy Policy and/or Terms and Conditions would appropriately satisfy this provision. The attributes of "clear, concise, consumer-friendly, and prominent" within the Principle are entirely subjective, and consequently all but impossible to police. ZAAZ recommends restating these as objectively as possible: The policies should be made available on the site generally (at minimum via hyperlink), and specifically on the page where information is being actively provided for site-side targeting. Regarding the actual substance of the policies, ZAAZ recommends relying on recommendations already created by the FTC[11] and other consumer advocacy groups.[12, 13]

414 OLIVE WAY, SUITE 500 SEATTLE, WA 98101

[7] 45 C.F.R. § 164.500–164.534 (2001).
[8] 15 U.S.C 6809
[9] 15 U.S.C. § 1681 et seq
[10] 15 U.S.C. § 6501–6506
[11] Federal Trade Commission. (n.d.). *Fair Information Practice Principles.* Retrieved January 14, 2008, from Federal Trade Commission: http://www.ftc.gov/reports/privacy3/fairinfo.shtm
[12] TrustE. (2004). *Your Online Privacy Policy.* Retrieved January 14, 2008, from TrustE.org: http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf

ZAAZ

414 OLIVE WAY, SUITE 500 SEATTLE, WA 98101

Businesses should continue to have a legal ability to offer free goods and services in exchange for the right to market to customers in a targeted manner as consideration. The Principles defined by the FTC should not preclude companies from entering into this type of arrangement with their customers, providing the terms of the exchange are available to the customer prior to the marketing, and a means to end the relationship (e.g., via opt-out) exists.

While the above Principle adequately addresses the concerns regarding site-side targeting, they are inapplicable to ad-side targeting. With ad-side targeting, a visitor's path throughout the Internet is being tracked via a third party network, and not from the site itself. Therefore, no single site, unaffiliated with the network itself, can provide an adequate opt-out mechanism. It is incumbent upon the ad networks themselves to continue to provide Internet users with a means to exclude themselves from targeting. To date, the Network Advertising Initiative (NAI), a consortium of 14 of the largest ad networks, have jointly created a Behavioral Targeting equivalent of the Do Not Call List, where consumers can both see which networks are targeting them and opt out of them individually or en masse.[14] The FTC must understand that this type of Behavioral Targeting, where a consumer's visit history can be accessed by multiple parties, offers the greatest potential for misuse, and should aid the networks in compliance and enforcement wherever possible. ZAAZ recommends partnering with the NAI to publicize the opt-out procedures of ad-side Behavioral Targeting for the benefit of consumers.

Principle #2 - Reasonable security, and limited data retention, for consumer data

"Any company that collects and/or stores consumer data for behavioral advertising should provide reasonable security for that data. Consistent with the data security laws and the FTC's data security enforcement actions, such protections should be based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company."

Data security is a standard cost of doing business and any business, whether they operate online or offline, regardless of whether they engage in Behavioral Targeting, should adhere to best practices for the retention and protection of collected consumer data. Since ZAAZ believes that all businesses must meet this high standard, we do not recommend enacting any security recommendations specific to the practitioners of Behavioral Targeting.

Even without data security regulations, businesses have every economic incentive to be perceived as diligent protectors of consumer information. Companies who fail to provide adequate safeguards for customer information will be branded as untrustworthy and will fail accordingly. In fact, businesses that have attempted to take risks regarding what consumer information is shared[15] or how confidential information is secured[16] have met

---

[13] BBBOnline. (n.d.). *Sample Privacy Policy.* Retrieved January 14, 2008, from BBBOnline.org: http://www.bbbonline.org/privacy/sample_privacy.asp

[14] Netwok Advertising Initiative. (n.d.). *Opt Out of NAI Member Ad Networks*. Retrieved January 14, 2008, from networkadvertising.org: http://networkadvertising.org/managing/opt_out.asp

[15] See e.g., McCarthy, C. (2007, November 30). *Rough seas nearly sink Facebook's Beacon*. Retrieved January 14, 2008, from CNet News.com: http://www.news.com/8301-13577_3-9826664-36.html

ZAAZ

with considerable public outrage, class action lawsuits, and a significant loss of market share as a result.

Assessing the appropriate length of data retention is complicated by the fact that websites sell goods and services with wildly disparate sales cycles. An automotive retailer has a sales cycle measured in months and is rarely contacted thereafter for years following the sale. It would be perfectly reasonable for this retailer to maintain data on a consumer over the course of multiple visits throughout six to twelve months as the consumer seeks more relevant information about car features, incentives, and dealership availability. A music retailer online, however, has a much shorter, sometime instantaneous sales cycle, but may get return visits for further purchases that same day. To expect both businesses to adhere to a common principle of how long certain data types can be retained could grossly hinder both businesses in their attempts to cater to these vastly different and completely legitimate marketing scenarios.

Principle #3 - Affirmative express consent for material changes to existing privacy promises

"As the FTC has made clear in its enforcement and outreach efforts, a company must keep any promises that it makes with respect to how it will handle or protect consumer data, even if it decides to change its policies at a later date. Therefore, before a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. This principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data."

414 OLIVE WAY, SUITE 500 SEATTLE, WA 98101

ZAAZ concurs that all businesses online have an obligation to adhere to the contract to which the consumer agreed at the start of the business relationship. Should a business amend that agreement, it is the responsibility of the business to alert the consumer and to make every reasonable effort to outline the changes. This is a restatement of basic contract principles and should be applied to all aspects of online business, including how and whether Behavioral Targeting is employed.

Any changes within the agreement that specifically affects how a consumer's information is shared externally or handled internally must be communicated before the changes occur. While opt-in notification is encouraged, ZAAZ does not believe it must be essential to compliance, providing the mechanism for opting out of targeting and/or abrogating the business relationship entirely is made clear to the consumer before information is collected or shared in a new manner. Indeed, it is not uncommon for offline businesses such as banks, credit card companies and cell phone providers to alter the terms of an existing

[16] See e.g., Girard Gibbs LLP. (2007, August 15). *Class Action Lawsuit Filed Against Certegy Check Services and Fidelity National Information Services*. Retrieved January 14, 2008, from girardgibbs.com: http://www.girardgibbs.com/certegypressrelease.asp

ZAAZ

relationship purely through opt-out notification.[17] To require online companies specifically to engage in opt-in notification places an unfair burden on these businesses relative to offline competitors.

Principle #4 - Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising

"Companies should only collect sensitive data for behavioral advertising if they obtain affirmative express consent from the consumer to receive such advertising. FTC staff seeks specific input on (1) what classes of information should be considered sensitive, and (2) whether using sensitive data for behavioral targeting should not be permitted, rather than subject to consumer choice."

Outside of the data sets already protected by law, ZAAZ would consider all personally identifiable information to be sensitive data. Personally identifiable data is defined as "[data] that are associated with living persons, or that can be associated with living persons by deduction from personal identifiers in a data set."[18] It should be noted that personally identifiable data includes "confidential" data (e.g. social security numbers, bank information, etc.) but extends to any data that is linked definitively to an individual (e.g., country of residence, time of visit, etc.).

For ad-side Behavioral Targeting across multiple sites, ZAAZ recommends a prohibition against using personally identifiable pieces of information unless expressly consented to by the consumer in advance. If the behavior is collected in a manner that can be linked to a specific individual explicitly or through deduction, it must be anonymized before it is used across an ad network or a different site.

Conversely, for site-side Behavioral Targeting, the use of personally identifiable information is often a pre-requisite to doing business intelligently (e.g., retaining shipping address for purchase receipt), and often has perfectly legitimate offline equivalents. ZAAZ urges the FTC to refrain from regulating the use of personally identifiable information within the website where it was collected, provided again that the consumer has agreed to the Terms and Conditions and that the website is acting within the bounds of existing law.

Conclusion

ZAAZ is committed to a set of Principles regarding Behavioral Targeting that protects consumers while encouraging innovation. We would look forward to working with the Federal Trade Commission in any capacity to help further define the principles, and invite the FTC to contact us if we can provide additional information or services.

414 OLIVE WAY, SUITE 500 SEATTLE, WA 98101

[17] See e.g., Utility Consumers' Action Network. (n.d.). *Telecommunications: "Material Adverse" Clauses in Cell Phone Contracts*. Retrieved January 14, 2008, from ucan.org: http://www.ucan.org/telecommunications/wireless/material_adverse_clauses_in_cell_phone_contracts

[18] Harvard University. (n.d.). *Harvard University Information Security & Privacy : Glossary of Terms*. Retrieved January 14, 2008, from Harvard.edu: http://www.security.harvard.edu/glossary.php

About the Author

Jason Carmel is a Senior Optimization Manager for ZAAZ where he builds and executes strategic optimization, behavioral targeting, and personalization for clients such as Microsoft, Ford Motor Vehicles, Helio and Dell. Before ZAAZ, Mr. Carmel developed the web analytics and optimization programs for eFax.com as their Director of Marketing. Mr. Carmel is a member of the Bar in Maryland and received his J.D. from the Washington College of Law at the American University.

414 OLIVE WAY, SUITE 500 SEATTLE, WA 98101